What is claimed:

1. A method of managing reliance in an electronic transaction system, the method comprising the steps of:

(A) a certification authority issuing electronic signals representing a primary certificate to a subscriber;

(B) forwarding, from the certification authority to a reliance server, electronic signals representing information about the issued primary certificate;

(C) the reliance server maintaining the forwarded information about issued primary certificate;

(D) the subscriber forming a transaction and then providing electronic signals representing the transaction to a relying party, the transaction including electronic signals representing the primary certificate;

(E) the relying party sending to the reliance server electronic signals representing a request for assurance based on the transaction received from the subscriber;

(F) the reliance server determining whether to provide the requested assurance, said determining based on the information about the issued primary certificate and on the requested assurance; and, based on said determining,

(G) the reliance server issuing to the relying party electronic signals representing a secondary certificate providing the assurance to the relying party.

2. A method as in claim 1 wherein the primary certificate specifies a reliance limit and wherein the information forwarded by the certification authority to the reliance server includes electronic signals representing assurance parameters controlling whether the reliance server can provide assurance based on the primary certificate.

3. A method as in claim 2 wherein the assurance parameters include electronic signals representing an acceptable reliance limit in excess of the reliance limit specified in the primary certificate, and wherein the request for assurance is a request for reliance on a value in excess of the specified reliance limit, wherein the step (F) of the reliance server determining whether to provide the requested assurance comprises the step of:

(F1) determining whether the requested reliance would exceed the acceptable reliance limit.

4. A method as in claim 3 further comprising the step of:

(H) the reliance server tracking cumulative liability associated with the primary certificate, and

wherein the step (F1) of determining comprises the step of:

(F2) determining whether the requested reliance would cause the cumulative liability to exceed the acceptable reliance limit.

5. A method as in claim 2 wherein the requested assurance is for the accuracy of another certificate, and wherein step (F) further comprises the step of:

(F1) the reliance server checking the current validity and authenticity of the other certificate; and wherein the step (G) of issuing comprises the step of:

(G1) the reliance server issuing electronic signals representing the secondary certificate attesting to the accuracy of the other certificate.

6. A method as in claim 5 wherein the step (F1) of checking comprises the steps of:

verifying the other certificate's digital signature along a chain of certificates, and

checking whether the requested assurance is within the assurance parameters.

7. A method as in claim 2 wherein the requested assurance is for the authenticity of another certificate, and wherein step (F) further comprises the step of:

(F1) the reliance server checking authenticity of the other certificate; and wherein the step (G) of issuing comprises the step of:

(G1) the reliance server issuing electronic signals representing the secondary certificate attesting to the authenticity of the other certificate.

8. A method as in claim 7 wherein the step (F1) of checking comprises the steps of:

verifying the other certificate's digital signature along a chain of certificates, and

checking whether the requested assurance is within the assurance parameters.

9. A method as in claim 2 wherein the requested assurance is for the validity of another certificate, and wherein step (F) further comprises the step of:

(F1) the reliance server checking the current validity of the other certificate; and wherein the step (G) of issuing comprises

(G1) the reliance server issuing electronic signals representing the secondary certificate attesting to the validity of the other certificate.

10. A method as in claim 9 wherein the step (F1) of checking comprises the steps of:

determining whether the other certificate has been suspended, revoked, or has expired, and

checking whether the requested assurance is within the assurance parameters.

11. A method as in claim 2 wherein the requested assurance is for assurance of an agent's authority

and wherein step (F) further comprises the step of:

the reliance server returning electronic signals representing documentation of agency with an enveloping secondary certificate attesting to authenticity.

12. A method as in claim 11 wherein the documentation of agency includes a power of attorney.

13. A method as in claim 2 wherein the requested assurance is for assurance of a of person's accreditation

and wherein step (F) further comprises the step of:

the reliance server returning a statement by a licensing or professional body regarding the person's accreditation, with electronic signals representing an enveloping secondary certificate attesting to the statement's authenticity.

14. A method as in claim 2 wherein the requested assurance is for assurance of existence and/or good standing of entity and wherein step (F) further comprises the step of:

the reliance server returning electronic signals representing a statement by a public office in which the entity is incorporated indicating that the entity exists, is in good standing, and is qualified to conduct business, wherein statement is enclosed in the secondary certificate attesting to the statement's authenticity.

15. A method as in claim 2 wherein the requested assurance is for assurance of the performance of an obligation and wherein step (F) further comprises the step of:

the reliance server issuing electronic signals representing a statement of assurance of payment, wherein statement is enclosed in the secondary certificate attesting to the statement's authenticity.

16. A method as in claim 1 further comprising the steps of:

(I) the reliance server and the relying party entering into a contract prior to the reliance server issuing the secondary certificate.

17. A method as in claim 16 wherein the contract is entered into after the relying party makes its request.

18. A method as in claim 2 wherein the transaction includes electronic signals representing a digital signature and wherein the assurance parameters include electronic signals representing a maximum supplemental assurance that can be issued for a particular digital signature.

19. A method as in claim 2 wherein the assurance parameters include electronic signals representing at least one of:

a maximum supplemental assurance that can be issued in a single secondary certificate;

a maximum supplemental assurance that can be issued to any particular relying party;

a maximum supplemental assurance that can be issued during one or more specified time intervals;

a maximum number of secondary certificates that can be issued on the primary certificate;

a maximum time period during which a secondary certificate may remain valid;

a maximum reliance limit that can be listed in a secondary certificate valid for a specified transaction type;

specific information that must be submitted by the relying party along with its request in order to provide a basis for the supplemental assurance;

an amount of supplemental assurance that the subscriber has prepaid and restrictions on how that prepaid assurance can be issued in a secondary certificate;

a requirement that the subscriber approve issuance of supplemental assurance by the reliance server for a secondary certificate to be issued to the relying party before a relying party's request for a secondary certificate can be granted;

thresholds which trigger a report being sent from the reliance server to the certification authority;

how often the reliance server should report to the certification authority about the extent of supplemental assurance issued on the primary certificate;

signals representing restrictions limiting disclosure of or access to the primary certificate to specified parties;

requirements that the transaction be signed by additional parties besides the subscriber, optionally specify who those additional parties are and what number of them must sign;

a scale of the amount of supplemental assurance that can be issued based on the number and identity of additional parties that sign; and

information regarding the validity of the primary certificate.

20. A method as in claim 19 wherein an assurance parameter can be restricted to a particular time period.

21. A method as in claim 20 wherein the particular time period is the entire period during which the primary certificate is valid.

22. A method as in claim 19 wherein the specific information includes electronic signals representing some of a specific class of certificate that has been promised to the relying party, specification of a transaction type and a second signature.

23. An electronic transaction system comprising:

a certification authority issuing electronic signals representing primary certificates to subscribers to the system; and

a reliance server connectable to the certification authority and receiving from the certification authority electronic signals representing information regarding the primary certificates issued by the certification authority, the reliance server issuing, upon request from relying parties, electronic signals representing secondary certificates to the relying parties, the issuing being based on the information provided by the certification authority and on information provided by the relying parties.

24. A system as in claim 23 further comprising:

at least one other party connectable to the reliance server, wherein the reliance server provides the electronic signals representing he secondary certificate to the other party prior to issuing the electronic signals representing the secondary certificate to the relying party.

25. A system as in claim 23 wherein the reliance server digitally signs the secondary certificate prior to issuing it to the relying party.

26. In an electronic transaction system in which a certification authority issues electronic signals representing digital certificates to subscribers, a method of automatic replacement of a

subscribers certificate, the method comprising the steps of, by a subscriber:

(A) creating a standby application for certification of a new key pair;

(B) digitally signing the standby application with a private key and then destroying the private key;

(C) including electronic signals representing the public key corresponding to the private key in a transactional certificate valid only for the standby application and forwarding the transactional certificate to the certification authority; and, by the certification authority,

(D) keeping electronic signals representing the transactional certificate; and subsequently,

(E) the subscriber sending electronic signals representing the standby application to the certification authority;

(F) the certification authority verifying the digital signature on the application by reference to the transactional certificate; and then

(G) issuing electronic signals representing a new time-based certificate listing the public key indicated in the standby application.

27. A method of managing reliance in an electronic transaction system in which subscribers have digital time-based certificates issued by certification authorities, the method comprising the steps of, by a relying party:

receiving electronic signals representing a transaction from a subscriber, the transaction including information regarding at least one time-based certificate of that subscriber;

creating a message based on certificate information from the transaction, the message specifying an amount of the transaction upon which the relying party intends to rely; and

sending electronic signals representing the message to a reliance server requesting a guarantee for the amount of the transaction upon which the relying party intends to rely.

28. A method as in claim 27 further comprising the steps of, the relying party:

receiving electronic signals representing a voucher from the reliance server in response to the step of sending the message; and

continuing the transaction with the subscriber based on information in the voucher.

29. A method of managing reliance in an electronic transaction system in which subscribers have digital time-based

certificates issued by certification authorities, the method comprising the steps of, by a reliance server:

receiving electronic signals representing a reliance request message from a party, the message specifying an amount of a transaction upon which the party intends to rely and requesting a guarantee for the amount of the transaction, the message including certificate information derived from the transaction;

determining whether to provide a guarantee for the amount of the transaction; and

sending electronic signals representing a voucher to the relying party, the voucher including an indication of whether the reliance server guarantees the amount of the transaction.

30. A method as in claim 29 wherein the step of determining further comprises the step of:

determining whether certificates associated with the transaction have been revoked or suspended.

31. A method as in claim 30 further comprising the steps of:

receiving from the certification authority electronic signals representing an actual reliance limit for a certificate;

storing the actual reliance limit; and

determining whether the requested amount would exceed the actual reliance limit.

32. A method as in claim 31 further comprising the step of maintaining a cumulative liability for a certification authority.

33. A method of managing reliance in an electronic transaction system, the method comprising the steps of, by a certification authority:

issuing electronic signals representing a time-based certificate to a subscriber, the certificate specifying a stated reliance limit; and

forwarding to a reliance server electronic signals representing an actual reliance limit for the certificate, the actual reliance limit being different from the stated reliance limit.

34. A method of managing reliance in an electronic transaction system in which subscribers have digital certificates, the method comprising the steps of, by a relying party:

receiving electronic signals representing a transaction from a subscriber, the transaction including information regarding at least one certificate of that subscriber;

creating electronic signals representing a message based on certificate information from the transaction, the message specifying an aspect of the transaction upon which the relying party intends to rely; and

sending the electronic signals representing the message to a reliance server requesting a guarantee for the aspect of the transaction upon which the relying party intends to rely.

35. A method as in claim 34 further comprising the steps of, the relying party:

receiving electronic signals representing a reply receipt from the reliance server in response to the step of sending the message; and

continuing the transaction with the subscriber based on information in the reply receipt.

36. A method as in claim 34 wherein some of the subscriber's certificates have associated fees, the method further comprising the step of, the reliance server:

ascertaining a fee for its services based on the fees of certificates associated with the transaction.

37. A method as in claim 36 wherein the fees include usage fees, guarantee fees and lookup fees.

38. A method as in claim 35 wherein the message requested certificate status checks and the reply receipt indicates whether the certificate status checks were acceptable.

39. A method as in claim 35, wherein the receipt indicates whether the reliance server guarantees the aspect of the transaction upon which the relying party intends to rely.

40. A method as in claim 34 wherein the aspect of the transaction upon which the relying party intends to rely specifies a monetary value and the receipt indicates whether the reliance server guarantees the transaction for that monetary value.

41. A method as in claim 40 wherein the reliance server bases its guarantee on information specified in a certificate associated with the transaction.

42. A method of managing reliance in an electronic transaction system in which subscribers have digital certificates, the method comprising the steps of, by a reliance server:

receiving electronic signals representing a message from a party thereby requesting a guarantee for an aspect of the transaction, the message including certificate information derived from the transaction;

validating information in the message to determine whether to provide the guarantee for the aspect of the transaction; and

sending electronic signals representing a reply receipt to the relying party, the reply receipt including an indication of whether the reliance server guarantees the aspect of the transaction.

43. A method as in claim 42 wherein the step of validating further comprises the step of:

determining whether certificates associated with the transaction have been revoked or suspended.

44. A method as in claim 43, wherein the certificate information included in the message includes unique identifiers for certificates associated with the transaction, and wherein the step of determining comprises the step of:

looking up unique certificate identifiers on certificate revocation lists.

45. A method as in claim 43, wherein the step of determining is performed based on previously obtained information about certificates.

46. A method as in claim 43 wherein the aspect of the transaction for which a guarantee is requested is a monetary reliance value, and wherein at least one certificate associated with the transaction specifies a monetary limit, the step of validating further comprising the steps of:

determining whether the monetary reliance value is within the monetary limit specified in the certificate.

47. A method as in claim 46, wherein the step of determining further comprising the steps of:

obtaining a value of a current cumulative monetary liability for the certificate;

determining whether the sum of the monetary reliance value and the current cumulative monetary liability would exceed the specified monetary limit; and, based on this determining,

updating the current cumulative monetary liability.

48. A method of managing reliance in an electronic transaction system, the method comprising the steps of:

a certification authority issuing electronic signals representing a time-based certificate to a subscriber;

forwarding, from the certification authority, electronic signals representing information about the certificate to a reliance server, the information including a unique identifier for the certificate and an actual reliance limit for the certificate;

the subscriber forming electronic signals representing a transaction based on the certificate and forwarding the transaction to a relying party;

the relying party sending electronic signals representing a reliance request message to the reliance server concerning the transaction;

the reliance server checking information in the reliance request message, and, based on the checking;

issuing electronic signals representing a transactional certificate as a voucher to the relying party.

49. A method as in claim 48 wherein the time-based certificate includes a stated reliance limit which is zero.

50. A method as in claim 48 wherein the certificate states that reliance on the certificate can only be made if the certificate is checked with a reliance server.

51. A method as in claim 50 wherein the certificate specifies the reliance server.

52. A method as in claim 50 further comprising the step of the reliance server digitally signing the transactional certificate.

53. A method as in claim 50 further comprising the steps of, by the reliance server:

forwarding the electronic signals representing the transactional certificate to at least one other party;

receiving the electronic signals representing the transactional certificate from another party; and

digitally signing the transactional certificate.

54. A method as in claim 53 further comprising the step of the other party digitally signing the transactional certificate.

55. A method as in claim 48 wherein the reliance request message specifies an amount of the transaction upon which the relying party intends to rely.

56. A method as in claim 55 wherein the step of checking comprises the step of determining whether the specified amount would exceed the certificate's actual reliance limit.